dispatch
Internet-Draft
Intended status: Informational
Expires: 1 June 2026

L. Zhang
Huawei Technologies
N. Geng
Huawei
X. Shang
Q. Gao
Z. Li
Huawei Technologies
J. Ge
CAICT

28 November 2025

Enhanced A2A Requirements for Agents Collobration in Enterprise
draft-zgsgl-dispatch-a2a-requirements-enterprise-01

Abstract

This document proposes enhanced requirements for the A2A protocol tailored to enterprise applications.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 1 June 2026.

Copyright Notice

Table of Contents

1. Introduction

With the widespread adoption of AI technologies, AI agents with special expertise are are developed and applied to everywhere in our life. However, there are some tasks that are too complict to be finished by a signle agent. The collobration of different agents are necessary. Google Cloud launched the Agent2Agent (A2A) open protocolaiming to provide a unified standards for agents collaboration. However it still faces numerous challenges when applied to enterprise scenarios.

This document proposes enhanced requirements for the A2A protocol tailored to enterprise applications.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Motivation

With the widespread adoption of AI technologies, AI agents with special expertise are are developed and applied to everywhere in our life, such as translation agents, image processing agents, and chartting agents. However, there are some tasks that are too complict to be finished by a signle agent. The collobration of different agents are necessary. Against this backdrop, Google Cloud

launched the Agent2Agent (A2A) open protocol on April 9, 2025, aiming to provide a unified standards for agents collaboration.

Although the A2A protocol has provided a foundational framework for multi-agent collaboration, it still faces numerous challenges when applied to enterprise scenarios.

* Lack of centralized agent discovery capabilities: Centralized agent discovery offers significant advantages for internal agent collaboration in terms of data consistency, controllability, and deployment complexity in a enterprise. However, the A2A protocol still lacks a well-defined interface for centralized directory services. In addition, the number of agents within enterprises is growing rapidly. Large enterprises often deploy hundreds of specialized agents covering various domains such as finance, human resources, R&D, and operations. The increasing number of agents poses new challenges to the latency and accuracy of agent discovery.

* Complex business processes: In actual enterprise operations, core business processes are often highly complex. For example, tasks such as end-to-end risk control and approval in the financial industry, or supply chain coordination and scheduling in manufacturing, often need to be broken down into dozens of interrelated subtasks. These involve multiple steps, including data verification, logical judgment, and cross-departmental resource scheduling. Temporary agent collaboration groups need to be created based on task requirements, and conflicts between different subtasks are common, requiring the agent communication protocol to have mechanisms for temporary group creation and conflict resolution.

* Strict permission control: Enterprises have extremely stringent requirements for agent permission control. On one hand, they need to assign differentiated permissions based on data sensitivity (e.g., customer privacy data, core business secrets) and task types to prevent unauthorized access. On the other hand, they need to trace the entire interaction history of agents to meet compliance and audit requirements. This poses new challenges to the granularity of permission control and the auditing capabilities of the protocol.

This document proposes enhanced requirements for the A2A protocol tailored to enterprise applications, based on the challenges mentioned above in enterprise scenarios.

3. Enhanced Requirements for A2A

3.1. Enhanced Discovery Requirements

* Interfaces for agent communication with centralized directory services: The interfaces for agent communication with centralized directory services should be supported to provide agent registration, addressing, and enable capability-based agent discovery.

* Optimized centralized directory services: It is required to support concurrent collaboration of thousands or more agents, reducing search latency for massive numbers of agents within large enterprises.

* Enhanced intent-based discovery and matching capabilities: The directory service should be able to map high-level user intents to chains or combinations of agents capable of fulfilling these intents.

3.2. Enhanced Collobration Requirements

* Conflict resolution mechanism: The conflict resolution mechanism should be added to define rules for agents to resolve conflicts in outcomes and data inconsistencies, reducing the need for manual intervention.

* Temporary collaboration group creation mechanism: The temporary collaboration group creation machanism allows agents to form temporary teams on demand to complete complex tasks, which will automatically disband after task completion.

* Task progress reporting mechanism: The task progress reporting mechanism permits remote agents to regularly report progress percentages, providing visibility and control over the task execution process.

3.3. Enhanced Security Requirements

* Fine-grained permission control: The fine-grained permission control mechanism allows collaboration permissions to be assigned based on task type and data level to prevent unauthorized access.

* Collaboration behavior audit log: The collaboration behavior audit log mechanism records the entire process of agent interactions to support traceability and compliance verification.

4. IANA Considerations

This document has no IANA actions.

5. Acknowledgements

6. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Authors' Addresses

Li Zhang
Huawei Technologies
No. 156 Beiqing Road
Beijing
China
Email: zhangli344@huawei.com

Nan Geng
Huawei
Beijing
China
Email: gengnan@huawei.com

Xiaotong Shang
Huawei Technologies
No. 156 Beiqing Road
Beijing
China
Email: shangxiaotong@huawei.com

Qiangzhou Gao
Huawei Technologies
No. 156 Beiqing Road
Beijing
China
Email: gaoqiangzhou@huawei.com

Zhenbin Li
Huawei Technologies
No. 156 Beiqing Road
Beijing
China
Email: robinli314@163.com

Jian Ge
CAICT
52 Huayuan North Road
Beijing
China
Email: gejian@caict.ac.cn